

## UNITED STATES DISTRICT COURT

RICHARD W. NAGEL  
CLERK OF COURTfor the  
Southern District of Ohio

2019 MAY -9 PM 4:37

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)iPhone SE assigned call number 937-304-8099 and  
International Mobile Subscriber Identity Number (IMSI)  
number 310120242722519

Case No.

3:19mj270-11

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
See Attachment A-4located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):  
See Attachment B-4

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

See Attachment C-4

Offense Description

The application is based on these facts:  
See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R Kinzig

Applicant's signature

Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 5-9-19

City and state: Dayton, Ohio

Sharon L Ovington

Judge's signature

Sharon L. Ovington, U.S. Magistrate Judge

Printed name and title

**ATTACHMENT A-4**

**DESCRIPTION OF PERSON TO BE SEARCHED**

iPhone SE assigned call number 937-304-8099 and International Mobile Subscriber Identity Number (IMSI) number 310120242722519 (“TARGET CELL PHONE-1”).

This warrant authorizes the forensic examination of the TARGET CELL PHONE-1 for the purpose of identifying the electronically stored information described in Attachment B-4.

**ATTACHMENT B-4**

**LIST OF ITEMS TO BE SEIZED AND SEARCHED**

Items evidencing violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography); and 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), including but not limited to the following:

1. Any visual depictions and records related to the possession, attempted possession, receipt, attempted receipt, distribution, and attempted distribution of child pornography.
2. Any images or videos of child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any Internet history indicative of searching for child pornography.
5. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed and/or traded.
6. Any Internet or cellular telephone communications (including email, social media, etc.) with minors.
7. Evidence of utilization of the Kik messenger application.
8. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
9. Lists of computer and Internet accounts, including user names and passwords.
10. Any information related to Internet Protocol (IP) addresses and Wi-Fi accounts accessed by TARGET CELL PHONE-1.
11. Any information related to the use of aliases.
12. Any GPS, mapping, and location information.
13. Any records, documents, and billing records pertaining to accounts held with telephone, electronic, and Internet service providers.

14. Evidence of user attribution showing who used or owned TARGET CELL PHONE-1 at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.



**ATTACHMENT C-4**

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS**

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

**INTRODUCTION**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents and investigators of the Homeland Security Investigations (HSI) and FBI, I am currently involved in an investigation of child pornography and child exploitation offenses committed by **STEPHEN E. KIRBY II**. This Affidavit is submitted in support of Applications for search warrants for the following:
  - a. The residential property located at 5068 Nielson Court, Huber Heights, Ohio, 45424 (hereinafter referred to as the "**SUBJECT PREMISES**" and more fully described in Attachment A-1 hereto);
  - b. The person of **STEPHEN E. KIRBY II** (hereinafter referred to as "**KIRBY**" and more fully described in Attachment A-2 hereto);
  - c. 2015 Nissan Altima bearing Ohio license plate 661YTM and Vehicle Identification Number (VIN) 1N4AL3AP3FC247454 (hereinafter referred to as "**SUBJECT VEHICLE**" and more fully described in Attachment A-3 hereto);
  - d. iPhone SE assigned call number **937-304-8099** and International Mobile Subscriber Identity Number (IMSI) number 310120242722519 (hereinafter referred to as "**TARGET CELL PHONE-1**" and more fully described in Attachment A-4 hereto); and
  - e. iPhone 7 Plus assigned call number **937-684-5792** and International Mobile Equipment Identity (IMEI) number 355376083197462 (hereinafter referred to as "**TARGET CELL PHONE-2**" and more fully described in Attachment A-5 hereto).
3. The purpose of the Applications is to seize evidence of violations of the following:

- a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess child pornography; and
  - b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce.
4. The items to be searched for and seized are described more particularly in Attachments B-1 through B-5 hereto and are incorporated by reference.
5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the **SUBJECT PREMISES**, the person of **KIRBY**, the **SUBJECT VEHICLE**, **TARGET CELL PHONE-1**, **TARGET CELL PHONE-2**, and the Computer and Electronic Media (as defined in Attachments B-1 through B-5) located at the **SUBJECT PREMISES**, on the person of **KIRBY**, in the **SUBJECT VEHICLE**, on **TARGET CELL PHONE-1**, and on **TARGET CELL PHONE-2**.
7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime, contraband, fruits of crime, or other items illegally possessed, property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1), are present at the **SUBJECT PREMISES**, on the person of **KIRBY**, in the **SUBJECT VEHICLE**, on **TARGET CELL PHONE-1**, on **TARGET CELL PHONE-2**, and on the Computer and Electronic Media (as defined in Attachments B-1 through B-5) located at the **SUBJECT PREMISES**, on the person of **KIRBY**, in the **SUBJECT VEHICLE**, on **TARGET CELL PHONE-1**, and on **TARGET CELL PHONE-2**.

#### **PERTINENT FEDERAL CRIMINAL STATUTES**

8. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or



through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

9. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
10. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
11. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

### **BACKGROUND INFORMATION**

#### **Definitions**

12. The following definitions apply to this Affidavit and Attachments B-1 through B-5 to this Affidavit:
  - a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

- b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
- c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
- e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- f. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).



- g. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- h. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- i. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- j. A **“Smartphone”** is a mobile cellular telephone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access, and an operating system capable of running downloaded applications.
- k. **Wi-Fi** is a technology that allows electronic devices to connect to a wireless LAN network. Devices that use Wi-Fi technology include personal computers, video game consoles, smartphones, digital cameras, tablets, and modern computers.
- l. The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Kik Messenger Application

13. Kik is a cross-platform instant messenger application available on smartphones. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content.
14. The Kik messenger application is administered by Kik Interactive Inc., a company based in Ontario, Canada. The application can be downloaded free of charge from the Internet. It requires a smartphone with either a data plan or access to a Wi-Fi network to use.
15. Unlike many other smartphone instant messenger applications that are based on a user's telephone number, Kik uses usernames to identify its users. Each user selects and is assigned a unique user name for use on Kik's platform. Each user also creates a user profile, which includes a first and last name and an email address. Kik Interactive Inc. does not verify this information, and as such, users can provide inaccurate information.
16. Kik Interactive Inc. maintains users' profile information and collects IP addresses utilized by users to access the account and transmit messages. In some circumstances, Kik Interactive Inc. also collects users' dates of birth as well as other information about how users have used the messenger application. Kik Interactive Inc. will only release current information to law enforcement pursuant to service of proper legal service (typically profile information and IP addresses for the past thirty days, or the most recent thirty days if the account has not been recently used). Kik Interactive Inc. does not store or maintain chat message content.
17. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize the Kik messenger application to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of child pornography offenders believe that the Kik messenger application is a secure means of trading child pornography.
18. Kik Interactive Inc. has developed procedures to monitor and identify Kik accounts that may be utilized to commit child pornography and/or child abuse offenses. Kik Interactive Inc. typically reports any accounts that are identified to the Royal Canadian Mounted Police. The Royal Canadian Mounted Police typically refers information about any accounts that appear to utilize Internet service in the United States to agents of the Homeland Security Investigations (HSI).

Telegram Messenger

19. Telegram Messenger is a cloud-based instant messaging and voice over IP service that was developed by Telegram Messenger LLP, a privately-held company registered in



London, United Kingdom. The application can be downloaded and used free of charge on smartphones, tablets, and computers.

20. Telegram Messenger allows users to exchange messages, photographs, videos, and files of any type. Users can also create groups for up to 200,000 people or channels for broadcasting to unlimited audiences. In addition, Telegram allows users to make voice calls to other users.
21. Messages and media in Telegram are client-server encrypted and stored on servers by default. Telegram's special "secret" chats use end-to-end encryption, leaving no trace of the chats on Telegram's servers. The secret chats provide users the option to self-destruct messages and prohibit users from forwarding the messages. When users set the self-destruct timer on secret messages, the messages will disappear from both the sender's and receiver's devices when the timer expires.
22. Telegram users have the option to create a user name that is displayed to other users. User names are uniquely assigned on a first-come, first-serve basis.
23. Based on my training and experience, I know that individuals involved in child pornography and child abuse offenses have utilized Telegram Messenger to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of offenders utilize Telegram's security features to avoid detection from law enforcement officers.

#### Cloud Storage

24. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations. The following terms relate to the use of cloud computing:
  - a. "Cloud" is a generic term that refers to a network where the physical location and inner workings are abstracted away and unimportant to the usage. "The cloud" was first used to describe telecommunication networks, where the consumer was blissfully unaware of the inner workings of how their telephone conversation was transmitted to the remote end. The term was later used to describe computer networks, and ultimately to describe the Internet specifically. Knowing the physical location of a website is unimportant to using that service. Cloud computing also takes advantage of this definition of cloud, as it is also a service connected to a network, often the Internet. However, cloud computing offers specific services whereby customers rent remote computing resources such as processing power or data storage, and provision those resources themselves.

- b. “Cloud computing” is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
  - c. “Cloud Service Provider” (CSP) is the entity that offers cloud computing services. CSP’s offer their customers the ability to use infrastructure, platform, or software as a service. These services may include offerings such as remote storage, virtual machines, or Web hosting. Service is billed as a utility based on usage. CSP’s maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, account application information, and other information both in computer data format and in written record format. CSP’s reserve and/or maintain computer disk storage space on their computer system for the use of the cloud service subscriber for both temporary and long-term storage of electronic data with other parties and other types of electronic data and files. Such temporary, incidental storage is defined by statute as “electronic storage,” and the provider of such a service is an “electronic communications service” provider. A cloud service provider that is available to the public and provides long-term storage services to the public for electronic data and files, is providing a “remote computing service.” CSP’s may be able to provide some of the following, depending on the type of services they provide: NetFlow, Full Packet Captures, Firewall and Router Logs, Intrusion Detection Logs, Virtual Machines, Customer Account Registration, Customer Billing Information.
25. Dropbox is an on-line file hosting service operated by Dropbox Inc., a company headquartered in San Francisco, California. Dropbox accounts provide users with cloud storage, file synchronization, personal cloud, and client software. Dropbox creates a special folder on the user’s computer, and the contents of the folder are synchronized to Dropbox Inc.’s servers and to other computers and devices onto which the user has installed Dropbox, keeping the same files up-to-date on all devices. Users are provided 2 GB of free storage space for basic accounts.
  26. Mega is a cloud storage and file hosting service offered by Mega Limited, an Auckland-based company. Mega is known for its security feature where all files are end-to-end encrypted locally before they are uploaded. This encryption prevents anyone from accessing the files without knowledge of the pass key.
  27. Dropbox and Mega provide its users with the ability to share files or folders with others. One means of sharing files or folders is by creating a “sharing link”. A sharing link



creates a URL to store the file(s) or folder(s) so that others can access, view, and/or download them. These sharing links can be sent to others via email, Facebook, Twitter, instant message, or other means. Users can limit who can access their sharing links by setting passwords and/or expiration dates for the links.

28. Based on my training and experience, I know that individuals with large collections of child pornography files may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement. Furthermore, individuals often utilize sharing links to their cloud storage accounts to share child pornography files with others.

#### Gigatribe

29. GigaTribe is a freeware program that allows users to create their own private Peer-to-Peer network of contacts. To use GigaTribe, users download the free program and then select which folder(s) on their computer they want to share. Users do not automatically share files when using GigaTribe. File sharing is limited only to other users who have been added to one's private network via a "friends" request. Acceptance of a friend request permits that user to access and download files from the initiator of the request only, and vice versa; therefore each user is his/her own network administrator.
30. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize Gigatribe and other Peer-to-Peer applications to obtain and share child pornography files.

#### Cellular Telephone Data

31. Sprint Corporation and Verizon are companies that provide cellular telephone access to the general public. I know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.
32. Based on my training and experience, I know that Sprint Corporation and Verizon can collect cell-site data about **TARGET CELL PHONE-1** and **TARGET CELL PHONE-**



2. I also know that Sprint Corporation collects Per Call Measurement Data (PCMD), and Verizon collects Range to Tower (RTT) data. Both PCMD and RTT data capture the time it takes for a signal to travel from the tower to the handset and back again. Based on this time, the network will provide a distance between the tower and cell phone. Furthermore, I know that wireless providers such as Sprint Corporation and Verizon typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

#### Common Abbreviations

33. Based on my training and experience, I know that individuals frequently use abbreviations or acronyms when communicating with each other on messenger applications such as Kik. Some of these abbreviations or acronyms include the following (as seen later in the Affidavit):
- a. Dau – Daughter
  - b. Diff - Different
  - c. Gf – Girlfriend
  - d. Lol – Laugh out loud
  - e. Perv – Pervert
  - f. Ppl – People
  - g. U – You
  - h. Ur – Your
  - i. Vid – Video
  - j. Yng - Young
  - k. YO – Years old

#### FACTS SUPPORTING PROBABLE CAUSE

##### Background Information of KIRBY

34. During the 2011 through 2013 time period, the FBI and Moraine (Ohio) Police Department investigated **KIRBY** for child pornography offenses. The investigation determined that **KIRBY** utilized the Gigatribe Peer-to-Peer file sharing program to trade child pornography files with others, and that he utilized both the Gigatribe Peer-to-Peer file sharing program and the Yahoo Messenger application to discuss the sexual exploitation and sexual abuse of children with various other users. As part of the investigation, a search warrant was executed at **KIRBY**'s residence in Moraine, Ohio. Over 16,000 images and over 300 videos of child pornography were recovered from **KIRBY**'s electronic devices that were seized pursuant to the warrant.
35. On or around May 7, 2012, **KIRBY** was arrested pursuant to a federal arrest warrant for

one count of possession of child pornography (in violation of 18 U.S.C. § 2252(a)(4)(B)) and one count of distribution of child pornography (in violation of 18 U.S.C. § 2252(a)(2) and (b)). On or around May 17, 2013, **KIRBY** pled guilty to one count of distribution of child pornography. On or around November 13, 2013, **KIRBY** was sentenced to 60 months imprisonment and five years of supervised release.

36. **KIRBY** was released from prison and entered a halfway house on or around January 9, 2018. On or around April 23, 2018, **KIRBY** was released from the Bureau of Prisons' custody and began his five-year term of supervised release. He is currently supervised by Probation Officer (PO) Christopher Owens of the United States Probation Service in Dayton, Ohio. As part of the conditions of his supervised release, **KIRBY** is prohibited from possessing or using any computer or device with access to any on-line computer service at any location without prior written approval of his probation officer. PO Owens authorized **KIRBY** to utilize an email account to search for jobs, provided that **KIRBY** only accessed the account from a public library. Otherwise, **KIRBY** is prohibited from having any electronic accounts or accessing Internet data from his cellular telephone or any other electronic devices.
37. **KIRBY** has reported to PO Owens that since he was released from the Bureau of Prisons' custody, he has lived with his grandmother (who will be referred to for purposes of this Affidavit as "Adult Female A") at the **SUBJECT PREMISES**. Pursuant to the terms of **KIRBY**'s supervised release, PO Owens has conducted multiple home visits at the **SUBJECT PREMISES**. PO Owens' first home visit was on or around May 15, 2018, and his most recent home visit was on or around May 1, 2019. PO Owens typically notified **KIRBY** in advance of the dates and times of these home visits.
38. **KIRBY** has also reported to PO Owens that he utilizes an iPhone bearing telephone number **937-684-5792 (TARGET CELL PHONE-2)**. Again pursuant to the terms of **KIRBY**'s supervised release, PO Owens has regularly reviewed the contents of **KIRBY**'s cellular telephone. PO Owens has not observed any child pornography files, evidence of utilization of an Internet browser, or evidence of utilization of messenger applications on this device. PO Owens has also reviewed the contents of the email account that **KIRBY** was authorized to utilize for job searches. PO Owens has not observed any child pornography files in this email account.
39. PO Owens described **KIRBY**'s vehicle as being a Nissan or Mazda sedan-style vehicle. PO Owens has seen **KIRBY** drive this vehicle on past occasions. PO Owens' description of the vehicle is generally consistent with the **SUBJECT VEHICLE**.
40. As part of his conviction, **KIRBY** is required to register as a sex offender. **KIRBY** completed his registration paperwork on or around April 24, 2018, and he renewed the registration paperwork on or around May 21, 2018 and November 13, 2018. On the paperwork for the initial registration and two renewals, **KIRBY** identified that he resided at the **SUBJECT PREMISES**. As part of his registration renewal on or around November 13, 2018, **KIRBY** reported that he worked at a business in Vandalia, Ohio.



41. Records from the Ohio Bureau of Motor Vehicles identified that **KIRBY** utilizes the **SUBJECT PREMISES** on his current Ohio driver's license. Records from the Ohio Bureau of Motor Vehicles also identified that the **SUBJECT VEHICLE** is presently registered to **KIRBY**'s father, STEPHEN KIRBY I. Records from the Montgomery County (Ohio) Auditor's website identified that the **SUBJECT PREMISES** is presently owned by Adult Female A and **KIRBY**'s grandfather. **KIRBY**'s grandfather is deceased.

Account Identified by Kik Interactive Inc.

42. In or around June 2018, as part of its ongoing monitoring of accounts (as detailed above in paragraph 18), Kik Interactive Inc. identified that a Kik account with an account name of mymister2018 was involved in a group chat that may have discussed child pornography and/or child abuse material. Excerpts from this group chat, as well as subscriber information for the mymister2018 Kik account, was provided to the Royal Canadian Mounted Police. After determining that the mymister2018 Kik account appeared to utilize Internet service in the United States, the Royal Canadian Mounted Police turned over the information to HSI agents. In April 2019, I obtained these records from HSI.
43. Based on the records provided by Kik Interactive Inc., the name of the group chat that the mymister2018 account user participated in was "Bi,Gay boys for Daddys(18?+ only)". Also based on records provided by Kik Interactive Inc., the group chat occurred on or around June 8, 2018. It appeared that Kik Interactive Inc. only provided small excerpts of this chat. These excerpts included the following:

mymister2018:	Had a boss used to tell me all about her sons puberty and erections. He was hot too <Conversation Break>
Kik User 2:	U have link DropBox and Mega?
Kik User 2:	Lots of stuff if you d <Conversation Break>
mymister2018:	Post in here
Kik User 2:	<i>Submits URL containing apparent sharing link to a Dropbox account.</i> <Conversation Break>
Kik User 2:	Send me link please
mymister2018:	Let me get into my email that has them all.

44. Based on my training and experience, I know that individuals involved in child pornography offenses often trade child pornography files by exchanging sharing links to files in their cloud storage accounts. I also know that child pornography offenders sometimes store lists of their sharing links in Word files, Text files, and draft email

messages. Based on the comment made by the mymister2018 account user about a boy experiencing puberty, it appeared that the Kik users in the above noted group chat were discussing children. Based on the contents of the conversation as well as other information detailed in the Affidavit (including information detailed below), it is reasonable to believe that the Dropbox link posted by Kik User-2 may possibly have contained child pornography or child erotica files. It is also reasonable to believe that the user of the mymister2018 Kik account had an email account that he/she might have utilized to store sharing links to files in his/her cloud storage account(s), possibly to include child pornography and/or child erotica files.

45. The subscriber information provided by Kik Interactive Inc. for the mymister2018 account included the following:
  - a. Kik Interactive Inc.'s records identified that a Kik account with an account name of mymister2018 and a profile name of "My Mister" was created on or around May 31, 2018. The email address mymister2018@yahoo.com was associated with the account profile.
  - b. Kik Interactive Inc. provided a log of IP addresses utilized to access the mymister2018 account during the approximate time period of May 31, 2018 through June 8, 2018. These records identified that IP addresses associated with Verizon's cellular telephone network were utilized to access the account and transmit messages on approximately 139 occasions. The use of IP addresses associated with Verizon's network is consistent with someone using the data plan of his/her cellular telephone to access the Internet. Four other IP addresses serviced by Charter Communications were also utilized to access the account and transmit messages: 71.79.52.128 (utilized on approximately 133 occasions), 75.186.19.61 (utilized on approximately 49 occasions), 74.142.189.50 (utilized on approximately five occasions), and 24.166.11.92 (utilized on approximately three occasions).
  - c. Kik Interactive Inc.'s records identified that an iPhone was used to access the mymister2018 account on or around June 5, 2018.

FBI Undercover Investigation – Kik Platform, December 2018 to January 2019

46. In December 2018 and January 2019, agents and task force officers of the Washington, D.C. Field Office of the FBI were involved in an ongoing online investigation to identify individuals utilizing social media and texting applications to commit child exploitation offenses. As part of the investigation, an undercover officer who will be referred to for purposes of this Affidavit as "UCO-1" routinely chatted with individuals who UCO-1 met on various social media applications.
47. On or around December 29, 2018 and January 2, 2019, UCO-1 chatted via Kik Messenger with the yourmister2018 Kik account user. Below is a summary of this chat:



- a. The yourmister2018 account user indicated that he was 36 years old, was from Ohio, and had children who were 15 years old, 14 years old, and six years old.
  - i. I know that **KIRBY** was 36 years old at the time of this chat. I have also determined that **KIRBY** has two biological children and one step-child who were approximately 15 years old, 14 years old, and six years old at the time of the chat.
- b. UCO-1 purported that he engaged in sexual activities with his children, and he inquired if the yourmister2018 account user did the same. The yourmister2018 account user responded by stating: "Working on the 6 yo. Active some with a 10 and diff 6 yo. Was active with my teens when they were 2-5 but stopped. Got several other teens thiugh. You got videos of you".
  - i. Based on this response and the context of the conversation, it appeared that the yourmister2018 account user was indicating that he engaged in sexual activities with children. It also appeared that the yourmister2018 account user was soliciting UCO-1 for videos of UCO-1 engaging in sexual activities with his children.
- c. The yourmister2018 account user inquired about Telegram groups of which UCO-1 was aware.
- d. The yourmister2018 account user stopped communicating with UCO-1 on or around December 29, 2018, after stating that he was "out in public". UCO-1 re-initiated the conversation on or around January 2, 2019 and called the yourmister2018 account user "fake". The yourmister2018 account user responded by stating "Nah just don't trade my shot for free".
  - i. Based on my training and experience, I know that individuals involved in trading child pornography files often have quid pro quo relationships with their trading partners, and they often will not send files to others until they receive child pornography files from their trading partners. The above noted statement by the yourmister2018 account user is consistent with this practice. The statement is also consistent with someone who has access to child pornography files.

Information Provided by Cooperating Witness

48. In February 2019, an adult male who will be referred to for purposes of this Affidavit as "Adult Male A" reported to the Huber Heights (Ohio) Police Department that a person by the name of "Steve" was promoting and talking about having sex with children and infants. Adult Male A reported that he believed that "Steve" used the Kik account name



of yourmister2018 and lived at the **SUBJECT PREMISES**. Adult Male A provided the Huber Heights Police Department screen prints of iMessages<sup>1</sup> that he recently exchanged with “Steve”.

49. In April 2019, the Huber Heights Police Department forwarded me the report documenting the information provided by Adult Male A. I subsequently interviewed Adult Male A on several occasions. In summary, Adult Male A provided the following information:
- a. Around the fall of 2018, Adult Male A met “Steve” in a group chat on Kik Messenger. “Steve” used the Kik account name of yourmister2018. Adult Male A could not recall the name of this group chat but advised that it was for gay and bi-sexual men (which is consistent with the name of the group chat reported by Kik Interactive Inc., as detailed in paragraph 43).
  - b. After communicating via the group chat, Adult Male A and “Steve” communicated individually with each other on Kik Messenger. “Steve” utilized both the account names of yourmister2018 and yourmister2019. Adult Male A and “Steve” also communicated with each other via iMessages and telephone calls. “Steve” utilized telephone number **937-304-8099 (TARGET CELL PHONE-1)** for these communications. They communicated with each other for a period of a few months, ending in or around February 2019. They often talked to each other about sex and other sexually explicit topics.
  - c. Adult Male A and “Steve” met each other in person on a few occasions. They met in the garage of the **SUBJECT PREMISES** on approximately two to three of these occasions. “Steve” said that the **SUBJECT PREMISES** was his grandmother’s house, and he indicated that he did not live there.
  - d. On one occasion when they met in person, Adult Male A and “Steve” tried to guess each other’s names. When Adult Male A guessed the name “Steve”, “Steve” made an expression indicating that this was his name. According to Adult Male A, “Steve” never confirmed that it was his true name.
  - e. Sometime after the Christmas holiday, “Steve” said that he wanted to talk to Adult Male A via the Telegram application. Adult Male A created a Telegram account and communicated with “Steve”. Adult Male A could not recall “Steve’s” Telegram account name. During the communications, “Steve” sent Adult Male A one video and approximately three images of what appeared to be child pornography. Adult Male A stated that the images depicted what appeared to be the same female child posing nude. It did not appear to Adult Male A that

---

<sup>1</sup> iMessages is an instant messaging service developed by Apple Inc. The service allows Apple users to send text messages, documents, photographs, videos, contact information, and group messages over Wi-Fi, a cellular telephone’s data plan, or other forms of Internet access.

this child had experienced puberty. Adult Male A stated that the video depicted what appeared to be a female child performing sexual acts on a man. While it appeared to Adult Male A that the female depicted in the video was also a child, Adult Male A could not conclude with complete certainty that she was a child.

- f. “Steve” told Adult Male A that the female depicted in the images and video he sent via Telegram was a foster child with whom he had a sexual relationship. “Steve” did not specify the sexual acts he engaged in with the child or the child’s age. “Steve” also told Adult Male A that he had friends who brought children over to his house, and that he and the friends had sex with these children. “Steve” said that the children were as young as infants.
  - g. Shortly after receiving the suspected child pornography files, Adult Male A deleted the files and reported the communications to the Huber Heights Police Department.
  - h. Adult Male A provided a physical description of “Steve”. Adult Male A saw “Steve” drive a white Ford Fusion. Adult Male A also saw a Nissan Altima parked in the garage of the **SUBJECT PREMISES**. “Steve” stated that he worked in Vandalia, Ohio and had an iPhone.
    - i. I noted that Adult Male A’s description of “Steve” is mostly consistent with **KIRBY**’s physical description (although Adult Male A reported a different eye color and height than that of **KIRBY**).
    - ii. Based on records from the Ohio Bureau of Motor Vehicles, I know that there is a white Ford Fusion that is registered to Adult Female A at the **SUBJECT PREMISES**. Although Adult Male A recalled the Nissan Altima being a different color, the vehicle is consistent with the **SUBJECT VEHICLE**.
    - iii. As noted above in paragraph 40, **KIRBY**’s current sex offender registration paperwork identifies that he works in Vandalia, Ohio.
  - i. During one of the interviews, Adult Male A was shown a photographic line-up that depicted six white males, one of which depicted **KIRBY**. Adult Male A identified that **KIRBY** was “Steve”.
50. At the time that I interviewed Adult Male A in April 2019, he no longer had any of the messages he exchanged with “Steve” on his cellular telephone. However, I reviewed the screen prints that Adult Male A provided to the Huber Heights Police Department. Consistent with the information provided by Adult Male A, I noted that the iMessages included references to “Steve’s” alleged comments about having sex with infants. The iMessages also included a comment about the **SUBJECT PREMISES**. Adult Male A

also appeared to inquire about the alleged child pornography files that “Steve” previously sent. “Steve” indicated that he had these files available to show Adult Male A on a computer. Furthermore, “Steve” made comments indicating that he previously had an application on his cellular telephone that hid his files. Below are excerpts of the conversation:

Adult Male A: You’re sketch ab what’s on ur phone so you use that app to hide your shit and I’m saying that’s ok  
 Steve: I have no app anymore. My phone has been scrubbed. Not taking that risk anymore. New year. New me  
 Adult Male A: Scrub?  
 Steve: Cleaned  
 Adult Male A: Of what  
 Steve: That app that hide my files  
 Adult Male A: Why do you need to hide your files haha  
 Steve: You should send me stuff on Kik if you. Or you on here.  
 And because ppl use my phone  
 Adult Male A: But you saved those vids of that girl didn’t you  
 Adult Male A: Are those on a computer we could watch  
 Steve: I’ve created a perv haven’t I? Hehe  
 Adult Male A: Well??  
 Adult Male A: ??  
 Steve: Yea  
 Adult Male A: You still into that  
 Steve: Nope

.....

Adult Male A: You are a weirdo Steven  
 Steve: True and so are you  
 Adult Male A: You have had sex with infants  
 Steve: Have I? Oooooor was it a lie  
 Steve: Just to keep you wanting me  
 Adult Male A: 5068 Nielson ct. I can get you when ever I want  
 Steve: You could. Or I moved  
 Steve: Remember that wasn’t my house

Additional FBI Undercover Investigation – Kik Platform, April 2019

51. Based on the information provided by Adult Male A, UCO-1 contacted the user of the yourmister2019 Kik account on or around April 17, 2019. UCO-1 communicated with the yourmister2019 Kik account user on or around April 17, 2019 through April 18, 2019. Below is a summary of these communications via the Kik platform:

- a. In the communications, the yourmister2019 account user indicated that he had



teenage children. He further indicated that he did not currently engage in sexual activities with these children, but that he had engaged in sexual activities with other children.

- b. During the exchange of messages, the yourmister2019 account user sent UCO-1 one video file depicting child pornography. The yourmister2019 account user also requested images depicting UCO-1's purported child.
  - i. Based on the context of this conversation and other information noted in the Affidavit, it appeared that the yourmister2019 account user was soliciting child pornography files that depicted UCO-1 and his purported children.
- c. The yourmister2019 account user made a comment indicating that he had a second telephone at another location that contained more child pornography files.
- d. The yourmister2019 account user stated that he had "private" or "homemade" pornography at his home. The yourmister2019 account user described his "private" or "homemade" pornography as being files that depicted him and boys, as well as other fathers and their children.
  - i. Based on my training and experience, I know that offenders often refer to child pornography that they have produced as "private" or "homemade" pornography.
- e. Below is a transcript of UCO-1's chat with the yourmister2019 account user:

UCO-1:	Hey
UCO-1:	33 dad here with dau. You ?
yourmister2019:	Sons. Age? Active?
UCO-1:	Nice
UCO-1:	Yes mine is 8
UCO-1:	And I have a niece that's 3
UCO-1:	Yes active with daughter when she is asleep and active with 3 yo when I see her
UCO-1:	What about u how old is yours
yourmister2019:	Teens now so I don't get to play but I do have others. Hehe
UCO-1:	Nice !!!!
UCO-1:	What ages u have ?
yourmister2019:	Lots of different ones. Do you take requests or have stuff I can see
UCO-1:	I usually do live for live but if u have good yng newer stuff I might
yourmister2019:	I do. I go live randomly since I never know when I'll be

with a kid  
 UCO-1: Ah ok who u have access and age  
 yourmister2019: Ohio here  
 UCO-1: I can show I live real quick but can't do much right now  
 cause gf here  
 UCO-1: Va here  
 yourmister2019: Ok. I'm in bathroom. Go ahead  
 UCO-1: What u have in gallery now  
 yourmister2019: Not much since this is my public phone lol  
 UCO-1: Live stuff from past ? Or stuff from net?  
 UCO-1: Ah damn  
 UCO-1: Just want to know cool before I send lol  
 yourmister2019: *Sends close-up image of what appears to be a male's penis.*  
 UCO-1: Cock proves I'm not a cop lol  
 UCO-1: I mean I k or you're a dude lol  
 UCO-1: I know  
 UCO-1: U said u have different stuff but not on u now?  
 yourmister2019: Ya.  
 UCO-1: Ah ok  
 UCO-1: Well I'll be here for a while let me know when u do and we  
 can go from there  
 yourmister2019: You can't show live? like you said  
 yourmister2019: I found some videos but they aren't of me  
 UCO-1: That's fine  
 UCO-1: Yes  
 yourmister2019: Can I see something so I know your not a cop  
 UCO-1: Yes  
 UCO-1: *Sends image that depicts what appears to be the chest of  
 a female child wearing clothing (although the image does  
 not depict a real child). A man's hand is touching the  
 child's shirt.*  
 yourmister2019: Fuck wow  
 UCO-1: Yeah  
 yourmister2019: *Sends video file depicting the groin area of what appears to  
 be a white female child who is wearing underwear. What  
 appears to be a black male masturbates his penis. The  
 black male then pulls aside the child's underwear, exposing  
 her nude vagina. He rubs his penis on the child's nude  
 vagina and partially inserts his penis into her vagina. The  
 video is approximately 37 seconds in duration.*  
 UCO-1: I'm cool lol  
 UCO-1: Mmmmm  
 UCO-1: *Sends image that depicts what appears to be the chest of a  
 female child wearing clothing (although the image does not  
 depict a real child). A man's hand is pulling aside the*



*child's shirt, exposing her breast.*

yourmister2019: You got anything video of them or what can we do

yourmister2019: How young

yourmister2019: Is she

yourmister2019: Pussy?

UCO-1: She is 8 and yes I can do more

UCO-1: What else u have

yourmister2019: That's a video. Can I get one. I have others like that.  
Private stuff at home

UCO-1: Oh nice yes I can take a vid once I'm alone . Gf here now  
so had to sneak those.

UCO-1: Maybe a few more of yours and I'll try to sneak a vid

UCO-1: How old are your homemade stuff at home

yourmister2019: You don't have any saved?

yourmister2019: Of them?

UCO-1: Not the vids , I do live and erase. Been caught once and  
talked my way out of it so I'm careful

UCO-1: *Sends image that depicts what appears to be the abdomen  
of a female child wearing underwear and a shirt (although  
the image does not depict a real child). The child's shirt is  
pulled up, and part of her breast is exposed.*

UCO-1: ?

yourmister2019: Sorry. Ppl were around

yourmister2019: Hope I didn't lose you

UCO-1: No worries u scared me

UCO-1: Lol

yourmister2019: Nah. You know I'm real. I sent stuff

UCO-1: Yes . I sent u live so u know I'm legit lol

yourmister2019: Yes and hot

yourmister2019: Love to train her with you

UCO-1: Like i said I can get live vids once alone

UCO-1: Always wanted to see her with someone else be so hot

yourmister2019: Bet she sucks great coxk and will love it in her cunt and ass

UCO-1: Yes !

yourmister2019: You done that

UCO-1: Nor ads

UCO-1: Tip in pussy

UCO-1: Ass

yourmister2019: While awake

UCO-1: Mostly while she is asleep now

UCO-1: What others u have with u

yourmister2019: Couple younger

UCO-1: And what homemade stuff u have

UCO-1: Mmmmmm

yourmister2019: Mainly me with boys. Friends brothers. Couple other dads and theirs  
 UCO-1: Younger the better miss to baby/toddler days  
 UCO-1: Mmmm  
 UCO-1: Nice  
 yourmister2019: Oh  
 yourmister2019: You still near her  
 UCO-1: Can be  
 UCO-1: What else u have  
 yourmister2019: Videos of kids with men  
 UCO-1: Mmm  
 yourmister2019: Ya but how soon you wanna send some stuff. I need to get back. I'm in bathroom  
 UCO-1: Can u sent what u have to I did send live :)  
 yourmister2019: I sent a video though. I only have three or four on here. Trying to stretch them  
 UCO-1: Hmm  
 yourmister2019: Ok

Service of Administrative Subpoenas

52. On or around February 27, 2019 and April 19, 2019, administrative subpoenas were served to Charter Communications requesting subscriber information for the four IP addresses utilized to access the mymister2018 Kik account on a sample of dates and times that they were utilized to access the account and transmit messages (based on the records provided by Kik Interactive Inc., as detailed above in paragraph 45(b)). Records received from Charter Communications in response to the subpoenas provided the following information:
- a. The IP address of 71.79.52.128 (which was utilized to transmit approximately 133 messages for the mymister2018 Kik account) was subscribed to Adult Female A at the **SUBJECT PREMISES**.
  - b. The IP address of 74.142.189.50 (which was utilized to transmit approximately five messages for the mymister2018 Kik account) was subscribed to the Guest Inn-Suites at 800 West 8<sup>th</sup> Street, Cincinnati, Ohio.
  - c. Charter Communications no longer had records associated with the subscriber of the IP addresses 75.186.19.61 (which was utilized to transmit messages on approximately 49 messages for the mymister2018 Kik account) and 24.166.11.92 (which was utilized to transmit messages on approximately three messages for the mymister2018 Kik account), as the requested dates were past Charter Communications' retention period.
53. On or around September 10, 2018, an administrative subpoena was served to Verizon

requesting subscriber information for **TARGET CELL PHONE-2** (the telephone number that **KIRBY** reported having to PO Owens). Records received in response to the subpoena identified that the telephone number is subscribed to STEPHEN KIRBY at an address in London, Ohio. Based on this London, Ohio address, it appears that **KIRBY**'s father (STEPHEN KIRBY I) is the subscriber. Verizon's records indicated that the telephone number was activated on or around May 15, 2018 (shortly after **KIRBY** was released from the custody of the Bureau of Prisons).

54. On or around April 18, 2019, an administrative subpoena was served to Sprint Corporation requesting subscriber information and incoming/outgoing call and text message details for **TARGET CELL PHONE-1** (the telephone number Adult Male A used to communicate with "Steve"), as well as the make and model of the device that utilized this telephone number. Records received in response to the subpoena provided the following information:
- a. The telephone number was subscribed to "**STEVE KIRBY**" at 3150 Charlotte Mill Road, Dayton, Ohio. The account was activated on or around November 8, 2018 (approximately <sup>seven (only)</sup> seven months after **KIRBY** was released from the custody of the Bureau of Prisons), and it was active as of the date of the subpoena (on or around April 18, 2019).
    - i. The 3150 Charlotte Mill Road address is not listed on **KIRBY**'s driver's license or sex offender registration paperwork.
    - ii. I know that **KIRBY** resided at 3150 Charlotte Mill Road, Dayton, Ohio, prior to his arrest in 2012. Based on records from the Montgomery County (Ohio) Auditor, **KIRBY** currently owns this residence. Records from the Ohio Bureau of Motor Vehicles identified that **KIRBY**'s ex-wife presently utilizes this address on her current Ohio driver's license.
  - b. Consistent with the information provided by Adult Male A, the incoming/outgoing call and text message details identified that approximately five voice calls and approximately two text messages were exchanged between **TARGET CELL PHONE-1** and Adult Male A's telephone number during the approximate time period of February 16, 2019 through February 21, 2019.
    - i. It should be noted that because iMessages utilize Internet service to transmit messages, the iMessages do not appear on the incoming/outgoing text message details of the telephone provider. As such, the iMessages exchanged between Adult Male A and **KIRBY** are not reflected in the telephone records for **TARGET CELL PHONE-1**.
  - c. Consistent with the information provided by Adult Male A, Sprint Corporation's records identified that the device utilizing **TARGET CELL PHONE-1**'s



telephone number was an iPhone SE, gray in color. Sprint Corporation's records further identified that the device had an Electronic Serial Number of 089587943210027077 and International Mobile Subscriber Identity (IMSI) of 310120242722519.

55. On or around April 22, 2019, an administrative subpoena was served to the Quality Inn and Suites (which appears to be the new name for the Guest Inn-Suites) located at 800 West 8<sup>th</sup> Street in Cincinnati, Ohio, requesting information for any hotel stays by **KIRBY**. Records received in response to the subpoena indicated that **KIRBY** stayed at the hotel from the evening of June 6, 2018 through the morning of June 7, 2018. This time period covered the approximately five occasions in which the IP address subscribed to the Guest-Inn Suites was utilized to transmit messages for the mymister2018 Kik account (as detailed above in paragraph 45(b)).

#### Review of Kik and Telegram Profiles

56. On or around April 14, 2019 and May 9, 2019, I conducted an Internet search for publicly available Kik profiles. I located profiles for the mymister2018, yourmister2018, and yourmister2019 Kik accounts. The Kik account for mymister2018 account did not contain a profile picture, and it was not clear if the account was still active. I noted that the yourmister2018 and yourmister2019 Kik accounts utilized a profile name of "Your Mister" and the same profile picture – a picture of what appeared to be a person's wrist with the word "Always" tattooed on it. Both accounts (yourmister2018 and yourmister2019) appeared to presently be open and/or active. The use of the same profile picture, the same profile name, and nearly the same account name is consistent with the same person utilizing the yourmister2018 and yourmister2019 accounts (as reported by Adult Male A).
57. On or around May 9, 2019, an FBI investigator accessed publicly available information on Telegram Messenger. Consistent with information provided by Adult Male A, a Telegram account was located that was associated with **TARGET CELL PHONE-1**. This Telegram account had a user name of "yourmister2018" and a profile name of "Daddy Mister". The profile information indicated that the account was online as recently as May 9, 2019.

#### Location Information for **TARGET CELL PHONE-1** and **TARGET CELL PHONE-2**

58. On or around April 26, 2019, two search warrants were authorized by the United States District Court for the Southern District of Ohio authorizing (1) the release of historical subscriber information, incoming/outgoing call and text message transactional records, Internet connectivity data, and cell site information by Sprint Corporation for **TARGET CELL PHONE-1** for the time period of November 8, 2018 through April 26, 2019 and (2) the release of prospective location information (i.e., cell site, cell sector, and GPS information, commonly referred to as a "Ping Order") by Sprint Corporation for **TARGET CELL PHONE-1** for a period of 30 days. On or around April 29, 2019, two

additional search warrants were authorized by the United States District Court for the Southern District of Ohio authorizing (1) the release of historical subscriber information, incoming/outgoing call and text message transactional records, Internet connectivity data, and cell site information by Verizon for **TARGET CELL PHONE-2** for the time period of April 23, 2018 through April 29, 2019 and (2) the release of prospective location information (i.e., cell site, cell sector, and GPS information, commonly referred to as a “Ping Order”) by Verizon for **TARGET CELL PHONE-2** for a period of 30 days.

59. An FBI agent who has training and experience in examining cellular telephone data has conducted an initial review of the records of the historical records provided by Sprint Corporation for **TARGET CELL PHONE-1** (the telephone number Adult Male A used to communicate with “Steve” and that is associated with the Telegram account). In summary, the records provided the following information:
- a. Sprint Corporation’s records identified that only approximately 80 telephone calls and approximately 123 text messages were sent or received by **TARGET CELL PHONE-1** during the approximate time period of November 8, 2018 through April 26, 2019. Only approximately 18 of the 80 telephone calls contained call durations that were more than 60 seconds.
    - i. Based on this information, it does not appear that **TARGET CELL PHONE-1** was frequently utilized to make and receive telephone calls and text messages.
    - ii. Given the minimal call activity, there was not a lot of cell tower data to be used for analysis.
  - b. Although there was a fairly insignificant number of telephone calls and text messages, Sprint Corporation’s records identified that **TARGET CELL PHONE-1** accessed Internet data on thousands of occasions during the approximate time period of January 1, 2019 through April 26, 2019.
  - c. During the approximate time period of January 1, 2019 through April 26, 2019, **TARGET CELL PHONE-1** made or received telephone calls utilizing the closest cell tower to the **SUBJECT PREMISES** on approximately 11 occasions.
    - i. This information is consistent with **TARGET CELL PHONE-1** being at the **SUBJECT PREMISES** on these approximately 11 occasions. However, given the geographic area that the cell tower covers, the precise location of the device could not be determined.
    - ii. It should be noted that there were other occasions in which other cell towers near the **SUBJECT PREMISES** were utilized by **TARGET CELL PHONE-1** to make or receive telephone calls. Because cellular



telephones do not always utilize the closest cell towers, it is possible that **TARGET CELL PHONE-1** was at or near the **SUBJECT PREMISES** on these other occasions as well.

- d. Also during the approximate time period of January 1, 2019 through April 26, 2019, there were numerous occasions in which **TARGET CELL PHONE-1** accessed Internet data utilizing cell towers that cover the geographic area of Huber Heights, Ohio (consistent with the location of the **SUBJECT PREMISES**). For example, during the approximate time period of April 20, 2019 through April 26, 2019, **TARGET CELL PHONE-1** accessed Internet data on more than 600 occasions utilizing cell towers that cover the geographic area of Huber Heights, Ohio – many of which were during the overnight hours.
  - e. **TARGET CELL PHONE-1** did not access Internet data or make any telephone calls during the morning hours of April 18, 2019 (the time period when the yourmister2019 Kik account user communicated with and sent child pornography to UCO-1, as detailed above in paragraphs 51(a) through 51(e)).
    - i. This information, as well as other information detailed in the Affidavit, is indicative that **TARGET CELL PHONE-2** was utilized to communicate with UCO-1 on this date.
60. The prospective location information (“Ping Order”) for **TARGET CELL PHONE-1** was monitored during the approximate time period of April 29, 2019 through May 8, 2019. It should be noted that the location information provided by Sprint Corporation included degrees of uncertainty of up to approximately four and a half miles. As such, the precise locations of **TARGET CELL PHONE-1** could not be determined. It was noted that there were times throughout the day that **TARGET CELL PHONE-1** appeared to be powered off, and as such, no location information was available during those time periods. Below is a summary of location information for **TARGET CELL PHONE-1** during the times that it was turned on and location information was available:
- a. **TARGET CELL PHONE-1** was primarily in the geographic area of the **SUBJECT PREMISES** during the overnight hours.
  - b. **TARGET CELL PHONE-1** was consistently in the geographic area of **KIRBY**’s place of employment in Vandalia, Ohio during the morning and early afternoon hours on week days.
  - c. During the late afternoon hours of May 1, 2019, **TARGET CELL PHONE-1** was powered off. It was turned on throughout the morning and early afternoon hours, and after it was turned off, it was turned back on during much of the evening hours.
    - i. It was noted that the time period that the device was powered off



coincided with when PO Owens was conducting a home visit at the **SUBJECT PREMISES**. PO Owens informed me that he notified **KIRBY** in advance of the date and time of the home visit.

- ii. Based on this and other information noted in the Affidavit, it appears that **KIRBY** powered off **TARGET CELL PHONE-1** in an attempt to conceal it from PO Owens.
  - d. **TARGET CELL PHONE-1** was consistently in the same geographic location as **TARGET CELL PHONE-2** during times that both devices were powered on and location information was available. This information is consistent with the same person utilizing both devices.
  - e. **TARGET CELL PHONE-1** did not travel outside of the Southern District of Ohio.
61. An FBI agent who has training and experience in examining cellular telephone data has conducted an initial review of the records of the historical records provided by Verizon for **TARGET CELL PHONE-2** (the telephone **KIRBY** reported having to PO Owens). In summary, the records provided the following information:
- a. The device utilizing **TARGET CELL PHONE-2** was an Apple iPhone 7 Plus bearing IMEI number 355376083197462.
  - b. Verizon's records identified that **TARGET CELL PHONE-2** was regularly used to make and receive telephone calls and text messages during the approximate time period of May 15, 2018 through April 29, 2019. Verizon's records also identified that **TARGET CELL PHONE-2** accessed Internet data on thousands of occasions during the approximate time period of May 15, 2018 through April 29, 2019.
  - c. During the approximate time period of January 1, 2019 through April 26, 2019, **TARGET CELL PHONE-2** made or received telephone calls utilizing the closest cell tower to the **SUBJECT PREMISES** on more than 100 occasions.
    - i. This information is consistent with **TARGET CELL PHONE-2** being at the **SUBJECT PREMISES** on these more than 100 occasions. However, given the geographic area that the cell tower covers, the precise location of the device could not be determined.
    - ii. It should be noted that there were other occasions in which other cell towers near the **SUBJECT PREMISES** were utilized by **TARGET CELL PHONE-2** to make or receive telephone calls. Because cellular telephones do not always utilize the closest cell towers, it is possible that

**TARGET CELL PHONE-2** was at or near the **SUBJECT PREMISES** on these other occasions as well.

- d. On or around April 18, 2018, **TARGET CELL PHONE-2** made a telephone call at approximately 11:35 a.m. (which is in close proximity to when the yourmister2019 Kik account user communicated with and sent child pornography to UCO-1, as detailed above in paragraphs 51(a) through 51(e)). This telephone call utilized one of the cell towers that covers the geographic location of **KIRBY**'s place of employment in Vandalia, Ohio. Later in the day, at approximately 6:16 p.m., **TARGET CELL PHONE-2** made a telephone call using a cell tower that covers the geographic area of 3150 Charlotte Mill Road in Moraine, Ohio (the location where **KIRBY**'s ex-wife and presumably her and **KIRBY**'s children appear to reside, as detailed above in paragraph 54(a)(i)). During the late evening hours of April 18, 2019 and early morning hours of April 19, 2019, **TARGET CELL PHONE-2** made telephone calls utilizing cell towers that cover the geographic area of the **SUBJECT PREMISES**.
    - i. This cell tower data is consistent with **KIRBY** being at work when he communicated with UCO-1 and returning to the **SUBJECT PREMISES** later that night.
    - ii. As detailed above (in paragraphs 51(a) through 51(e)), the yourmister2018 Kik account user indicated in his communications with UCO-1 on April 18, 2019 that he was using his "public" phone, that he had another phone that had more child pornography files, and that he had access to more child pornography files (including "homemade" or "private" files) at his residence.
  - e. The cell tower data for **TARGET CELL PHONE-2** was compared to the cell tower data for **TARGET CELL PHONE-1** during the approximate time period of March 15, 2019 through April 26, 2019. Due to the minimal call activity for **TARGET CELL PHONE-1** (as detailed above in paragraph 58(a)), there were not many occasions when both devices were utilized during the same time periods. However, approximately four occasions were noted when **TARGET CELL PHONE-1** and **TARGET CELL PHONE-2** were utilized within relative close proximity to each other (i.e., less than two hours of each other). On these approximately four occasions, both telephones utilized cell towers that cover the same general geographic areas. These four occasions included one instance in which both telephones were utilized in the geographic area of the **SUBJECT PREMISES** and approximately three instances in which both devices were utilized in the geographic area of Beavercreek, Ohio. This information is consistent with the two devices being located at the same locations.
62. The prospective location information ("Ping Order") for **TARGET CELL PHONE-2** was monitored during the approximate time period of April 29, 2019 through May 8,



2019 (with the exception of the approximate time period of the afternoon hours of April 30, 2019 through the afternoon hours of May 1, 2019, during which time data was not collected due to an administrative error). It should be noted that the location information provided by Verizon included degrees of uncertainty of up to approximately three and six-tenths miles. As such, the precise locations of **TARGET CELL PHONE-2** could not be determined. Below is a summary of the prospective location information for **TARGET CELL PHONE-2**:

- a. **TARGET CELL PHONE-2** was primarily in the geographic area of the **SUBJECT PREMISES** during the overnight hours.
- b. **TARGET CELL PHONE-2** was consistently in the geographic area of **KIRBY**'s place of employment in Vandalia, Ohio during the morning and early afternoon hours on week days.
- c. **TARGET CELL PHONE-1** was consistently in the same geographic location as **TARGET CELL PHONE-2** during times that both devices were powered on and location information was available. This information is consistent with the same person utilizing both devices.
- d. **TARGET CELL PHONE-2** did not travel outside of the Southern District of Ohio.

#### Surveillance Activities

- 63. On or around May 2, 2019, an FBI agent observed the **SUBJECT VEHICLE** parked in the parking lot of **KIRBY**'s place of employment in Vandalia, Ohio. Location information for both **TARGET CELL PHONE-1** and **TARGET CELL PHONE-2** indicated that both devices were in this geographic location around the approximate time of the surveillance activity.
- 64. On the morning of on or around May 3, 2019, I observed the **SUBJECT VEHICLE** drive away from the **SUBJECT PREMISES** and travel in a direction consistent with traveling to **KIRBY**'s place of employment in Vandalia, Ohio. Approximately one-half hour later, I observed the **SUBJECT VEHICLE** parked in the parking lot of **KIRBY**'s place of employment. Location information for both **TARGET CELL PHONE-1** and **TARGET CELL PHONE-2** indicated that both devices were in the geographic locations of the **SUBJECT PREMISES** and then at the place of employment around the approximate times the approximate times of the surveillance activities.
- 65. During the late afternoon hours of on or around May 6, 2019, another FBI agent and I observed the **SUBJECT VEHICLE** parked in the parking lot of a fitness center in Beavercreek, Ohio. The other FBI agent also observed **KIRBY** inside this fitness center. Location information for **TARGET CELL PHONE-2** indicated that it was also in this



geographic location around the approximate time of the surveillance activity. **TARGET CELL PHONE-1** was powered off at the time of the surveillance activity, but it was powered on approximately one hour later. The location information for **TARGET CELL PHONE-1** at the time that it was powered on indicated that it was also in the geographic location of the fitness center.

66. On the morning of on or around May 9, 2019, another FBI agent observed a white male who resembled **KIRBY** exit the front door of the **SUBJECT PREMISES** and enter the detached garage. The agent then observed the **SUBJECT VEHICLE** exit the garage and drive away from the **SUBJECT PREMISES**. The FBI agent and I surveilled the **SUBJECT VEHICLE** as it traveled to **KIRBY**'s place of employment in Vandalia, Ohio. Location information for **TARGET CELL PHONE-2** indicated that the device was in the geographic locations of the **SUBJECT PREMISES** and then the place of employment around the approximate times of the surveillance activities. **TARGET CELL PHONE-2** was powered off at the time of the surveillance activity.

#### Conclusions Regarding Use of Accounts and Devices

67. As detailed above in paragraph 49(b), Adult Male A identified that he exchanged iMessages with "Steve" via **TARGET CELL PHONE-1**, and that "Steve" utilized two Kik accounts: yourmister2018 and yourmister2019. Adult Male A also identified that "Steve" had a Telegram account. As noted above, Adult Male A identified "Steve" via a photographic lineup as **KIRBY**. As detailed above in paragraphs 45 and 52(c), records from Kik Interactive Inc. and Charter Communications indicate that **KIRBY** also utilized a Kik account with the account name of mymister2018.
68. It was noted that the activation date for **TARGET CELL PHONE-1** (on or around November 8, 2018, as detailed in paragraph 54(a)) was after the date of the group chat reported by Kik Interactive Inc. (on or around June 8, 2018, as detailed in paragraph 43). As detailed above in paragraph 45(b), the records from Kik Interactive Inc. identified that the mymister2018 Kik account utilized Internet service associated with Verizon's network on a number of occasions to transmit messages. This information is consistent with the utilization of **TARGET CELL PHONE-2**, which is serviced by Verizon.
69. As detailed above in paragraph 51(e), the yourmister2019 Kik account user identified that he was using a "public" phone at the time he was communicating with UCO-1 on or around April 18, 2019. Based on the information detailed in the Affidavit, this statement is indicative that the yourmister2019 account user was utilizing **TARGET CELL PHONE-2** to communicate with and send a video file of child pornography to UCO-1. The yourmister2019 Kik account user indicated that he had another phone that had more child pornography files, and that he had access to more child pornography files at his residence. Based on this and other information noted in the Affidavit, it is reasonable to believe that **KIRBY** was referring to **TARGET CELL PHONE-1** when he mentioned his other telephone that contained child pornography files. Also based on this and other information noted in the Affidavit, it is reasonable to believe that the yourmister2019 Kik

account user utilized two cellular telephones (**TARGET CELL PHONE-1** and **TARGET CELL PHONE-2**) in furtherance of his child pornography activities.

70. As detailed above in paragraph 50, "Steve" indicated to Adult Male A that he had an application on his telephone that hid his files, and that he had the ability to "scrub" his telephone to remove files. Based on my training and experience, I know that child pornography offenders utilize various applications and techniques to hide their files. These applications and techniques can hinder law enforcement officers' ability to detect the files. Although PO Owens has not detected child pornography files on **TARGET CELL PHONE-1**, the comments made by "Steve" indicates that **KIRBY** utilizes one or more techniques to hide his files.
71. Based on all of the information detailed in the Affidavit, there is probable cause to believe that **KIRBY** is the user of the mymister2018, yourmister2018, and yourmister2019 Kik accounts; the yourmister2018 Telegram account; **TARGET CELL PHONE-1**; and **TARGET CELL PHONE-2**. There is also probable cause to believe that he has utilized the three Kik accounts, the Telegram account, and the two cellular telephones to possess, receive, and distribute child pornography and to discuss the sexual exploitation of children.
72. Also based on all of the information detailed above, there is probable cause to believe that **KIRBY** currently resides at the **SUBJECT PREMISES** and drives the **SUBJECT-VEHICLE**. Furthermore, there is probable cause to believe that **KIRBY** has utilized computer devices (to include **TARGET CELL PHONE-1** and **TARGET CELL PHONE-2**) at the **SUBJECT PREMISES**, on **KIRBY**'s person, and/or in the **SUBJECT VEHICLE** to access his Kik and Telegram accounts and to possess, receive, and distribute child pornography.

Evidence Available in Proposed Search Warrants

73. As further detailed below, I know that individuals typically maintain their cellular telephones on their persons, in their residences, and in their vehicles when they travel. Based on all of the information detailed in the Affidavit, there is probable cause to believe that **TARGET CELL PHONE-1** and **TARGET CELL PHONE-2**, as well as potentially other electronic media **KIRBY** has used in furtherance of his child pornography activities, are currently located at the **SUBJECT PREMISES**, on **KIRBY**'s person, and/or in the **SUBJECT VEHICLE**.
74. Based on my training and experience, I know that it is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices in furtherance of their child pornography and child exploitation activities. Individuals sometimes save their files to multiple devices to allow easy access to the files and/or to back-up the devices in case of a computer failure.



75. Again based on my training and experience, I know that collectors of child pornography often use external devices (such as thumb drives, external hard drives, CD's/DVD's, SD cards, SIM cards, etc.) to store child pornography. The accumulation of child pornography files may fill up the space on the hard drives of computers, and external devices are needed to store and maintain files. These devices also serve as a mechanism for transferring files from one computer to another. In my experience, individuals maintain such external devices in their residences. Given their portable size, individuals sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.
76. Based on my training and experience, I know that individuals are increasingly utilizing laptop computers and other smaller devices such as cellular telephones, iPads, and tablets to do their computing. These devices are typically maintained in the owners' residences. Due to their portable nature, individuals also sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.
77. Based on my training and experience, I know that collectors of child pornography often maintain their collections for long periods of time. In addition, computer evidence typically persists for long periods of time, and computer data can often be recovered from deleted space (as further detailed above).
78. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.
79. Also based on my training and experience, I know that individuals involved in child exploitation offenses utilize a variety of threats and manipulation techniques to compel their victims to engage or continue engaging in the illicit sexual activities (including the production of child pornography). These threats and manipulations are intended to control the victims and their activities, prevent them from stopping the activities, and prevent them from contacting law enforcement officers. It is common for such offenders to threaten that if the victims end the illicit sexual activities, the offenders will harm the victims and their family members and / or bring notoriety and shame to the victims by exposing the victims' involvement in the sexually explicit conduct.
80. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chatrooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others



about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

81. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the computer devices located at the offenders' residences, in their vehicles, and on their persons.
82. I know, in my experience, that individuals involved in child exploitation offenses sometimes print the pictures in hard copy format. Such individuals do so both for easier access / viewing of the files and to back-up the files in the event that one computer device becomes damaged and broken. Similarly, these individuals often save contact information (i.e., email addresses and account names) for those with whom they communicate about child exploitation offenses in multiple locations.
83. In addition, individuals often maintain lists of their electronic accounts (including associated user names and passwords) and their aliases in handwritten format. These papers are sometimes maintained in close proximity to their computers for easy access. In other cases, the papers may be hidden or maintained in secure locations to avoid detection by others.
84. In my experience, I know that many cellular telephones, iPads, and tablets store information related to IP addresses and Wi-Fi accounts that the telephone accessed and GPS data. This information helps in identifying the subjects' whereabouts during the criminal activities and the travels they took to get to these locations.
85. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers (such as Frontier Communications) often send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. Individuals often maintain these documents in their residences and/or on their computers. These documents can be materially relevant to investigations of child exploitation offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.

#### **ELECTRONIC STORAGE OF COMPUTER AND ELECTRONIC MEDIA**

86. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via

the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

87. There is probable cause to believe that things that were once stored on the Computer and Electronic Media (as defined in Attachments B-1 through B-5) recovered from the **SUBJECT PREMISES, KIRBY's person, the SUBJECT VEHICLE, TARGET CELL PHONE-1, and TARGET CELL PHONE-2** may still be stored there, for at least the following reasons:
- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
  - b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
  - c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
  - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."
88. As further described in Attachments B-1 through B-5, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Computer and Electronic Media (as defined in Attachments B-1 through B-5) recovered from the **SUBJECT PREMISES, KIRBY's person, the SUBJECT VEHICLE, TARGET CELL PHONE-1, and TARGET CELL PHONE-2** were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Computer and Electronic Media (as defined in



Attachments B-1 through B-5) recovered from the **SUBJECT PREMISES, KIRBY's** person, the **SUBJECT VEHICLE, TARGET CELL PHONE-1, and TARGET CELL PHONE-2** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

#### **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

89. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related



documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
  - b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.
90. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).
  91. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

#### **SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA**

92. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
  - a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a

preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

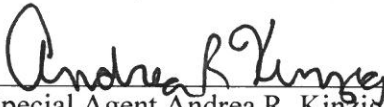
- b. On-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;
- c. Examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- d. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- e. Surveying various file directories and the individual files they contain;
- f. Opening files in order to determine their contents;
- g. Scanning storage areas;
- h. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachments B-1 through B-5; and
- i. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachments B-1 through B-5.

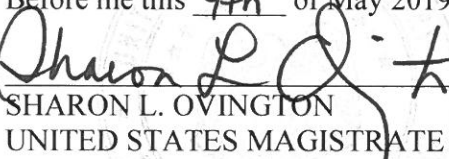
### CONCLUSION

93. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime, contraband, fruits of crime, or other items illegally possessed, property designed for use, intended for use, or used in committing a crime or violations of federal law, may be located at the **SUBJECT PREMISES**, on the person of **KIRBY**, in the **SUBJECT VEHICLE**, on **TARGET CELL PHONE-1**, on **TARGET CELL PHONE-2**, and on the Computer and Electronic Media (as defined in Attachments B-1 through B-5) located at the **SUBJECT**

**PREMISES**, on the person of **KIRBY**, in the **SUBJECT VEHICLE**, on **TARGET CELL PHONE-1**, and on **TARGET CELL PHONE-2**, including the following violations: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1).

94. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-5.

  
Special Agent Andrea R. Kinzig  
Federal Bureau of Investigation

SUBSCRIBED and SWORN  
Before me this 9th of May 2019  
  
SHARON L. OVINGTON  
UNITED STATES MAGISTRATE JUDGE